is the unused UTXO obtained as an account system, the total balance that Bitcoin users can use is obtained by summing up all UTXOs.

[0036] There are two sources of unspent in UTXO account:

[0037] (2.1) it is derived from part or all of a certain asset held in the user's own account of Account. While transferring these assets into the UTXO account system, the same type and quantity of digital assets will be correspondingly subtracted from the account of Account to ensure the validity of the initial source of UTXO in the entire system. The realization process has the following characteristics:

[0038] users can only initiate transfers from their own account of Account to their own UTXO account;

[0039] the transfer process is performed atomically;

[0040] (2.2) another method of obtaining is the transfer of UTXO from other users, which is equivalent to that the user as the recipient obtains a right to use or future ownership. The UTXO of the present invention adopts an unspent structure similar to the existing UTXO, but expands the parameters recorded by the UTXO and adds two time parameters, namely T1 and T2, thereby supporting the (N, M, T1, T2) model;

[0041] (3) segment operation of Time Lock:

[0042] (3.1) user A initiates a transfer operation from its own account of Account to UTXO about the digital assets (N, M) existing in the current account of Account, and passes in a parameter P, where p is the value of P and satisfies the condition of $ct<p<\infty$;

[0043] (3.2) deduct the corresponding digital asset (N, M) in user A's account of Account, and form a record of (N, M, ct, ∞) in UTXO, and according to the incoming parameter P=p, to execute

$$(N,M,ct,\infty)p=(N,M,ct,p)+(N,M,p+1,\infty)$$

thus, user A obtains a right to use the digital asset (N, M) in the time period [ct, p], and the future ownership of the digital asset (N, M) at the future time point p+1.

[0044] (4) Flow:

[0045] user A can transfer the formed (N, M, ct, p) and (N, M, p+1, ∞) respectively to UTXO accounts of different users.

[0046] among them, when user A transfers (N, M, p+1, ∞) to user B, it is equivalent to that user B obtains a future ownership of digital assets (N, M) at time point p+1, and user A will lose ownership of these assets.

[0047] (5) Judging the time attribute of UTXO:

[0048] when user B obtains a (N, M, p+1, ∞), he can choose to wait until $ct\geq p+1$, and he can directly obtain the ownership of (N, M).

[0049] Or user B can seek to obtain a right to use (N, M) with [T1, T2]=[ct, t'], as long as user B obtains $t'\geq p$, then user B can through

$$(N,M,ct,t')+(N,M,p-1,\infty)=(N,M,ct,\infty)$$

obtain current ownership of digital assets (N, M).

[0050] Similarly, users can obtain multiple [T1, T2] use rights of (N, M), as long as the time period [ct, p] is covered, the user can obtain the current right to use (N, M).

[0051] The judgment of the time attribute of UTXO will be done with the help of a filter for the time attribute of UTXO, this filter will determine whether the time parameter of UTXO meet the continuity of the target digital asset (N, M) in the time period [ct, ∞]. When the conditions are met, the UTXO with time attribute is converted into standard UTXO for operation.

[0052] (6) Time Lock merge operation

[0053] (6.1) User A is in his UTXO account, choose the continuous one that satisfies [ct,∞] in the relevant time period, a UTXO fragment on a digital asset (N, M), execute

$$(N,M,t,t')+(N,M,t'+1,\infty)=(N,M,t,\infty)$$

[0054] (6.2) at the same time, delete the related UTXO record in the UTXO record of user A (for example, by locking to a special target address), and increase the record of (N, M) in the user A's account Account.

[0055] This operation also needs to meet the following two requirements:

[0056] users can only merge Time Lock in their own UTXO and account of Account;

[0057] the above operation is completed atomically.

[0058] Using the method for performing segmenting locking and merging control of encrypted digital assets based on time dimension in this invention, through the processing of encrypted digital assets in the time dimension, not only can smart contracts or hash locking be used to realize the automated transfer of encrypted digital assets in the future, and the transferred encrypted digital assets can be transferred and traded before the set time (such as T2 of the present invention); at the same time, since the segmentation object of the present invention is based on the assets currently held by the user, therefore, the deterministic cash of future value rights and interests can ensure to be realize, and it has a wider range of applications.

[0059] In this specification, the present invention has been described with the reference to its specific embodiments. However, it is obvious still may be made without departing from the spirit and scope of the present invention, various modifications and transformation. Accordingly, the specification and drawings should be considered as illustrative rather than restrictive.

We claim:

1. A method for performing segmenting locking of encrypted digital assets based on time dimension, characterized in that, the said method comprises:

a first user terminal stores a first encrypted digital asset (N, M) in a first data structure which belongs to the first user terminal, and add attributes for a time period interval (T1, T2) of the first encrypted digital asset (N, M) to a second data structure which belongs to the first user terminal, in order to expand the first encrypted digital asset (N, M) into a second encrypted digital asset (N, M, T1, T2) having attributes for the time period interval (T1, T2); based on the second data structure, the first user terminal's ownership related to the first encrypted digital asset (N, M) in the time period interval (T1, T2) could be separated into the right to use of a second user terminal related to the first encrypted digital asset (N, M) in a time period interval (T1, P), and the first user terminal's ownership related to the first encrypted digital asset (N, M) in a time period interval (P+1, T2), the said T1, P, T2 are any positive integers, and the $T1<P<T2$.